AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Ryan P. Doyle, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Detective with the Newport Police Department ("NPD") and a Task Force Officer ("TFO") with the U.S. Drug Enforcement Administration ("DEA"). I have been a TFO since January 2021, and a Detective since 2014. Prior to becoming a Detective, I was a police officer with the Newport Police Department since 2007. As both a TFO and Detective, I have participated in investigations of narcotics trafficking and have conducted or participated in surveillances, the execution of search warrants, debriefings of informants and reviews of recorded conversations. Through my training, education, and experience, I have become familiar with the manner in which narcotics are packaged, distributed and transported. I am currently assigned to conduct investigations in the Providence District Office (PDO) of the DEA. I have prepared numerous affidavits in support of applications for State and Federal search warrants. My duties include the enforcement of federal criminal laws, including controlled substance violations and money laundering, under Titles 18 and 21 of the United States Code.

2. As a TFO with the DEA, I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses. I am a participating member of the PDO which is comprised of

personnel from the DEA and DEA Task Force Officers (TFOs) from the Providence Police Department, East Providence Police Department, Woonsocket Police Department, Cranston Police Department, NPD, North Kingstown Police Department, South Kingstown Police Department, Warwick Police Department, West Warwick Police Department, Central Falls Police Department, Coventry Police Department, Rhode Island State Police, Amtrak Police Department, and the Rhode Island State Attorney General's Office. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

3. I submit this affidavit in support of an application for the issuance of a search warrant authorizing the search of:

a. the SUBJECT PHONE 1, a blue iPhone with an unknown assigned call number, as more particularly described in Attachment A-1 (attached hereto and incorporated herein by reference), for the items described in Attachment B-1; and

b. the SUBJECT PHONE 2, a black Android cellular telephone with a metallic grey T-Mobile logo on the back and with an unknown assigned call number, as more particularly described in Attachment A-2 (attached hereto and incorporated herein by reference), for the items described in Attachment B-2.

4. For the reasons set forth below, I believe that KING is a drug trafficker who has used a cellular telephone to commit drug trafficking offenses. I submit that there is probable cause to believe that SUBJECT PHONE 1 and SUBJECT PHONE 2 (collectively, the SUBJECT PHONES) or other telephones used by him contain records and other evidence of the following offenses: conspiracy to distribute and possess with the intent to distribute more than 400 grams of fentanyl, in violation of 21 U.S.C. § 846; conspiracy to distribute and possess with the intent to distribute Xanax tablets (containing alprazolam, a schedule IV controlled substance), in violation of 21 U.S.C. § 846; possession with the intent to distribute more than 400 grams of fentanyl, in violation of 21 U.S.C. §§ 841 (a)(1) and (b)(1)(A); and possession with intent to distribute Xanax tablets (containing alprazolam, a schedule IV controlled substance), in violation of 21 U.S.C. §§ 841 (a)(1) and (b)(2) (collectively, the "TARGET OFFENSES"). More specifically, as will be discussed below, I submit that there is probable cause to believe that the cellular telephone(s) used by KING will contain evidence of the commission of a criminal offense or evidence which is contraband, the fruits of crime, or things otherwise criminally possessed, or which is designed or intended for use or which is or has been used as the means of committing an offense in violation of the TARGET OFFENSES.

Probable Cause

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement agents.

This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have also relied on information provided to the DEA by a Confidential Informant who I will only refer to as "CI-1." In order to protect CI-1's identity, I will refer to CI-1 with a masculine pronoun regardless of CI-1's gender.

6. CI-1 has been providing information to the government since May 2021. CI-1 has a criminal history which includes disorderly conduct and misdemeanor shoplifting. CI-1 also currently has three criminal cases pending: one Rhode Island State case for possession of a Schedule I to V controlled substance; one Massachusetts State case for Larceny over $1,200; and one Federal case before this Court for possession for one count of violating 21 U.S.C. §§ 841 (a)(1) and (b)(1)(B) and one count of violating 21 U.S.C. §§ 841 (a)(1) and (b)(1)(A). CI-1 also has a pending State case in Rhode Island for two counts of possession of a Schedule 1 to V controlled substance (oxycodone and clonazepam). CI-1 has previously cooperated with law enforcement, having served as an informant to Cranston Police. Since the start of his cooperation with the DEA, he has provided information that I or other law enforcement agents have independently corroborated through toll records, recorded conversations, video recordings, physical surveillance, and other law enforcement confidential sources. He has proven to be a credible and reliable informant. I have never found him to have provided false information.

7. CI-1 was previously a subject of an investigation I conducted in an undercover capacity. CI-1 informed me that he obtained pills via a supplier who he communicated with via the WhatsApp application. Based on my training and experience, WhatsApp is a messaging application primarily used on cellular telephones. CI-1 knew his dealer by his WhatsApp handle, "Poe," but also knew that his last name was King. CI-1 provided me with a screenshot of his WhatsApp conversation with Poe, showing a large quantity of pills.

8. DEA personnel arranged several controlled buys with "Poe" utilizing CI-1. "Poe" was later identified as KING after another DEA TFO recognized CI-1's description of "Poe" based on the TFO's knowledge of KING's from previous narcotics investigations. CI-1 was shown a photograph of KING and confirmed this identification.

9. On May 17, 2021, CI-1, under my supervision, called KING on his cell phone (phone number 401-644-0987) (hereinafter referred to as "KING Cell") and arranged for a controlled buy of approximately 2,000 Xanax (alprazolam) pills. KING agreed, and stated that he would be arriving at CI-1's residence at approximately 6:30 p.m.

10. Prior to the meeting, I searched CI-1 for contraband with negative results. At the agreed-upon time, a man who was later identified as Corey MARTINEZ (DOB xx/xx/1973) arrived at CI-1's residence driving a rental vehicle. MARTINEZ met with CI-1 in the rental vehicle, which was parked outside of CI-1's residence, and provided

CI-1 approximately 2,000 pills in exchange for $1,800. This transaction was not captured via video or audio surveillance due to a technical issue. I personally observed the transaction occur, although I did not specifically see the pills being passed to CI-1.

11. Following this transaction, law enforcement followed MARTINEZ, who drove to Mr. Bigg's Saloon in Johnston, RI where he met with KING. Law enforcement then followed KING from Mr. Bigg's Saloon to KING's residence of 175 Federal Way, Apartment 101, Johnston RI (the "Residence"). A records review of the rental vehicle driven by MARTINEZ showed that the address on file for this rental was the Residence.

12. The 2,000 pills sold to CI-1 were later sent out for laboratory analysis, and while the results are still pending, the pills are similar in shape and appearance to Xanax pills that have previously tested positive for alprazolam, a schedule IV controlled substance.

13. On May 25, 2021 CI-1 contacted KING via WhatsApp to arrange for a second controlled buy under my supervision for approximately 4,000 pills of fentanyl. KING stated that he would be sending his "auntie" to deliver the pills, who would be meeting CI-1 at CI-1's residence. Prior to the meeting, I searched CI-1 for contraband with negative results.

14. Shortly thereafter, a woman later identified as Erin SMITH (DOB xx/xx/1969) arrived at CI-1's residence in a white Nissan sedan and met with CI-1 in the Nissan. SMITH provided CI-1 approximately 4,400 pills (weighing approximately 764 grams) in exchange for $6,900. This transaction was captured via video and audio

surveillance. I personally observed the transaction occur, although I did not specifically see the pills being passed to CI-1.

15. Following this transaction, law enforcement followed SMITH, who stopped briefly at her residence before driving to a nearby barber shop, where she met KING. Law enforcement then followed KING, who drove to the Residence. The approximately 4,400 pills sold to CI-1 were sent out for laboratory analysis shortly thereafter and returned positive for fentanyl along with lidocaine.

16. On June 3, 2021, CI-1, under my supervision, contacted KING via WhatsApp to inquire whether CI-1 could purchase 1,000 pills of fentanyl. Prior to the meeting, I searched CI-1 and his vehicle for contraband with negative results. KING informed CI-1 that he was in South Kingston and would be driving to Johnston shortly.

17. Approximately an hour later, KING was seen arriving at the Residence in a rental vehicle. Shortly thereafter, KING walked over to Mr. Bigg's Saloon where he met CI-1. CI-1 purchased approximately 1,000 pills of fentanyl from KING for $2,000. This transaction was captured via audio and video recording, and I personally observed the transaction occur, though I did not specifically observe the pills being handed to CS-1.

18. The 1,000 pills sold to CI-1 were later sent out for laboratory analysis, and while the results are still pending, the pills are identical in appearance to the pills that were provided by SMITH on May 25, 2021 and which tested positive for fentanyl.

19. Following this third controlled buy, KING walked back to the Residence. Subsequent surveillance conducted at this address has revealed that a vehicle belonging to KING is occasionally parked outside this residence. KING and MARTINEZ have been observed entering and exiting the common area of the apartment complex as well.

20. On June 29, 2021, CI-1, under my supervision, contacted KING via WhatsApp to inquire whether CI-1 could purchase another 1,000 pills of fentanyl. KING informed CI-1 that he was at Mr. Bigg's Saloon and needed an hour to prepare. KING was then observed driving back to the Residence in his personal vehicle. Approximately two hours later, KING was seen departing the Residence in his vehicle.

21. Prior to meeting KING, I searched CI-1 and his vehicle for contraband with negative results. KING arrived at Mr. Bigg's Saloon in his vehicle, where he met CI-1. CI-1 purchased approximately 1,000 pills from KING for $2,000. This transaction was captured via audio and video recording, and I personally observed the transaction occur, though I did not specifically observe the pills being handed to CS-1. The 1,000 pills sold to CI-1 were later sent out for laboratory analysis, and while the results are still pending, the pills are identical in appearance to the pills that were provided by SMITH on May 25, 2021 and which tested positive for fentanyl.

22. In subsequent conversations with CI-1 using WhatsApp, KING stated that he has hundreds of thousands of pills for sale and possesses several kilograms of "Molly" (referencing 3,4-Methylenedioxymethamphetamine, or MDMA). KING also claimed that he has 1.2 million pills of Xanax.

23. On July 14, 2021 I applied for and received arrest warrants for MARTINEZ, KING, and SMITH. I also applied for and received search warrants for KING's person, vehicle, the Residence, and the KING Cell. KING, SMITH, and MARTINEZ were all apprehended in the late afternoon of July 19, 2021.

24. When KING's person was searched, the SUBJECT PHONES were found in a satchel that KING was carrying over his shoulder, along with approximately $6,750 in U.S. currency, and were subsequently taken into evidence. When the telephone number assigned to the KING Cell was called, neither phone rang. A search of KING's vehicle and the Residence failed to uncover the KING Cell.

Seizure of Electronic Devices

25. As described above, I believe that KING is engaged in the TARGET OFFENSES and that he is using a cellular telephone or telephones in the commission of the TARGET OFFENSES. Based on my training and experience, I believe probable cause exists that the SUBJECT PHONES and/or other electronic devices as described in Attachments B-1 and B-2 will contain evidence, fruits, and instrumentalities of the TARGET OFFENSES.

26. Based on my training and experience, I know that drug traffickers commonly use cellular telephones and/or smartphones to communicate about and further their drug trafficking activities, but are aware of law enforcement's use of electronic surveillance, and thus frequently change cellular telephone numbers and/or use multiple cellular phones at the same time, as well as prepaid cellular phones (where

the subscriber of the phone is not required to provide personal identifying information), in an effort to thwart law enforcement's use of electronic surveillance. Based on my training and experience, drug traffickers often use multiple phones and change their phone numbers frequently to avoid law enforcement detection. A cellular telephone is a handheld wireless device used for voice and text communication as well as for accessing the internet. Telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls and text messages made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet, including electronic mail ("email"), iMessages, Facebook Messages, WhatsApp messages, and other forms of electronic communications. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Based on my training, experience, and research, I know that many cellular telephones have capabilities described above. In my training and experience, examining data stored on

devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device as well as his criminal accomplices. I am also aware that drug traffickers often speak in vague, guarded, or coded language when discussing their illegal business in an effort to further prevent detection, and often use text messages in lieu of phone calls to avoid speaking over the telephone.

27. Additionally, based on my training and experience, the WhatsApp application – which KING utilized to communicate with CI-1 concerning narcotics transactions – can be installed on multiple cellular devices and is not bound to a single device like a call number.

28. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones and mobile phones can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

29. Based on my knowledge, training, experience, and information provided to me by other agents, I know that electronic files or remnants of such files can be recovered from smartphones and mobile phones months or years after they have been

written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their telephones, they can easily transfer the data from their old telephone to their new telephone.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a telephone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, an operating system may also keep a record of deleted data in a "swap" or "recovery" file

c. Wholly apart from user generated files, storage media—in particular, internal hard drives—contain electronic evidence of how the device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

30. Based on all of the information that I have obtained in the course of this investigation, and for the reasons more specifically set forth herein, I believe that KING used cellular telephones, including the SUBJECT PHONES, in the commission of the TARGET OFFENSES. I believe that KING uses smartphones and/or telephones to facilitate the TARGET OFFENSES, to communicate with drug suppliers, with customers

(including CI-1), and with co-conspirators (including MARTINEZ and SMITH), and that communications, records, appointments and other information will be found on their smartphones/telephones, and that their smartphones/telephones will be found on or near them. *See e.g., United States v. Feliz*, 182 F.3d 82, 87-88 (1st Cir. 1999).1

Biometric Access

31. The search warrant also requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant(s) I am applying for would permit law enforcement

[1] In *Feliz*, the First Circuit made clear that, in the drug trafficking context, evidence of drug transactions can be expected to be found in a drug trafficker's residence for months after evidence of the last transaction. 182 F.3d at 87 ("[C]ourts have upheld determinations of probable cause in trafficking cases involving [three months long] or even longer periods") (citing *United States v. Greany*, 929 F.2d 523, 525 (9th Cir. 1991) (two year-old information relating to marijuana operation not stale)). As the First Circuit has explained "[b]y its very nature, drug trafficking, if unchecked, is apt to persist over relatively long periods of time." *United States v. Nocella*, 849 F.2d 33, 40 (1st Cir. 1988).

personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the user's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the user's face with her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

d. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

Conclusion

32. Based on the facts contained in this affidavit, I believe there is probable cause to cause to believe that the requested search warrants will reveal evidence of Federal Offenses committed by KING, including, but not limited to the TARGET OFFENSES.

33. I, Ryan Doyle, having signed this Affidavit under oath as to all assertions and allegations contained herein, state that its contents are true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,

Ryan P. Doyle, Task Force Officer
Drug Enforcement Administration

Attested to by the applicant in accordance with the requirements of Fed.R. Crim. P. 4.1 by telephone.

_____	_____
Date	*Judge's signature*
_Providence, RI_____	Lincoln D. Almond, US Magistrate Judge
City and State	*Printed name and title*

ATTACHMENT A-1 (SUBJECT PHONE 1)
PHONE TO BE SEARCHED

The SUBJECT PHONE 1 is a blue iPhone with an unknown assigned call number and unknown serial number (SUBJECT PHONE 1).

ATTACHMENT B-1 (SUBJECT PHONE 1)
ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of 21 U.S.C. § 841(a)(1); and (b) conspiracy to possess with intent to distribute and/or distribute controlled substances, in violation of 21 U.S.C. § 846 (collectively, the "Specified Federal Offenses"):

1. Records and information[1] relating to the receipt, transport, storage, and/or sale of narcotics.

2. Records and information relating to banking and financial records of or relating to the SUBJECT PERSON[2] and any conspirators, including but not limited to Corey MARTINEZ DOB 04/29/1973 ("MARTINEZ") and Erin SMITH DOB 09/13/1969 ("SMITH") and their nominees, assignees, or co-conspirators, including but not limited to bank statements, deposit tickets, deposit items, checks, money orders, cashier's checks, official checks, bank drafts, wire transfer instructions and receipts, checkbooks, check registers, passbooks, withdrawal slips, credit memos, debit memos, signature cards, account applications, automatic teller machine receipts, safe deposit box applications, safe deposit box keys, pre-paid debit and credit cards, debit and credit card statements, charge slips, receipts, financial statements, balance sheets, income statements, cash flow statements, ledgers, journals, accounts receivable, accounts payable, leases, brokerage statements, and any other items evidencing the obtaining, disposition, secreting, transfer, or concealment of assets.

3. Records and information relating to the access and use of money service businesses, such as Western Union and/or Moneygram; online bank transfer services, such as Zelle, Venmo, or Paypal; and cryptocurrency accounts and cryptocurrency exchanges, such as BitCoin.

[1] As used in this Attachment, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks, backup drives, or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and digital and photographic form.

[2] The SUBJECT PERSON referred to is JONATHAN KING, DOB February 26, 1991.

4. Records and information relating to any communications by, between and among, and/or relating to the SUBJECT PERSON and any conspirators, including but not limited to SMITH and MARTINEZ, relating to the Specified Federal Offenses, including opening and access of bank accounts.

5. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show access, accounts with, and/or use of instant and social media messages (including Facebook, Facebook Messenger, Instagram, Pinterest, Snapchat, FaceTime, Skype, and WhatsApp), SMS and MMS text messages, iMessage, iCloud, and email accounts by the SUBJECT PERSON, and any conspirators, including but not limited to SMITH and MARTINEZ. Records and information showing communications by, between and among, and/or relating to the SUBJECT PERSON, and any conspirators, including but not limited to SMITH and MARTINEZ, that relate to the Specified Federal Offenses via any such accounts and communications platforms.

6. Records and information relating to Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations, including travel to banking locations.

7. Any records which document an association between and among the SUBJECT PERSON, and any conspirators, including but not limited to SMITH and MARTINEZ, including social media accounts, photographs, and video and audio recordings.

8. Records and information records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with any co-conspirators involved in the Specified Federal Offenses, including but not limited to SMITH and MARTINEZ, including calendars, address books, telephone or other contact lists, correspondence, receipts, and wire transfer or fund disposition records, and communications relating to the same.

9. All records or documents evidencing or relating to foreign or domestic travel of the SUBJECT PERSON, or co-conspirators, including but not limited to SMITH and MARTINEZ, including but not limited to airline tickets, tickets for other means of transport, credit card receipts, travel vouchers, hotel receipts, restaurant receipts, gas receipts, notes, schedules, other receipts evidencing travel, boarding passes, itineraries, luggage tags and receipts, frequent flyer statements and awards, car rental receipts and statements,

photographs of travel locations, maps, written directions to a location, visas, passports, United States and foreign customs declaration receipts and forms.

10. Records and documents reflecting the purchase or lease of real estate, and vehicles, precious metals, jewelry, or other items obtained with drug trafficking proceeds.

11. Identification cards, driver's license cards, passports, visas, and travel documents.

12. Records relating to the use, ownership, possession, and control of computers, tablets, cellular telephones, including but not limited to the SUBJECT PHONE 1, and/or other cellular and digital devices seized from the SUBJECT PERSON, internet service, or IP addresses associated with the SUBJECT PERSON;

13. For any computer, cellular or digital device, cellular telephone, and/or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information whose seizure is authorized by this warrant, including any cell phones (hereinafter, "DIGITAL DEVICE")[3]:

    a. evidence of who used, owned, or controlled the DIGITAL DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the DIGITAL DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
    e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;

[3] The term "DIGITAL DEVICE" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, external drives, RAM, flash memory, CD-ROMS, memory sticks, USB drives, and other magnetic or optical media.

f. evidence of the attachment to the DIGITAL DEVICE of other storage devices or similar containers for electronic evidence;
g. evidence of programs (and associated data) that are designed to eliminate data from the DIGITAL DEVICE;
h. evidence of the times the DIGITAL DEVICE was used;
i. passwords, encryption keys, and other access devices that may be necessary to access the DIGITAL DEVICE;
j. documentation and manuals that may be necessary to access the DIGITAL DEVICE or to conduct a forensic examination of the DIGITAL DEVICE;
k. records of or information about Internet Protocol addresses used by the DIGITAL DEVICE; and
l. records of or information about the DIGITAL DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

14. With respect to any and all electronically stored information in cellular telephones and cellular devices, in addition to the information described herein, agents may also access, record and seize the following:
a. Telephone numbers of incoming/outgoing calls stored in the call registry;
b. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
c. Any incoming/outgoing text messages relating to the above criminal violations;
d. Telephone subscriber information;
e. The telephone numbers stored in the cellular telephone and/or PDA;
f. Records relating to the use, possession, and control of any cellular telephones and cellular devices seized;
g. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including but not limited to photographs, videos, e-mail, and voice mail relating to the above Specified Federal Offenses.

15. Contextual information necessary to understand the evidence described in this attachment.

II. AUTHORIZED SEARCH PROCEDURE

1. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

2. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
   a. Any computer or storage medium capable of being used to commit further or store evidence of the Specified Federal Offenses; and
   b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

3. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

4. This warrant does not cover the search and seizure of any Digital Devices determined by agents to be used exclusively by third parties not involved with the Specified Federal Offenses.

III. SEARCH PROCEDURE FOR DEVICES CAPABLE OF BIOMETRIC ACCESS

1. During the execution of this search warrant, law enforcement is permitted to:
   a. depress the user's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and
   b. hold the device in front of the user's face with her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT A-2 (SUBJECT PHONE 2)
PHONE TO BE SEARCHED

The SUBJECT PHONE 2 is a black Android phone with a metallic grey T-Mobile logo on the back and with an unknown assigned call number and unknown serial number (SUBJECT PHONE 2).

ATTACHMENT B-2 (SUBJECT PHONE 2)
ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of 21 U.S.C. § 841(a)(1); and (b) conspiracy to possess with intent to distribute and/or distribute controlled substances, in violation of 21 U.S.C. § 846 (collectively, the "Specified Federal Offenses"):

1. Records and information[4] relating to the receipt, transport, storage, and/or sale of narcotics.

2. Records and information relating to banking and financial records of or relating to the SUBJECT PERSON[5] and any conspirators, including but not limited to Corey MARTINEZ DOB 04/29/1973 ("MARTINEZ") and Erin SMITH DOB 09/13/1969 ("SMITH") and their nominees, assignees, or co-conspirators, including but not limited to bank statements, deposit tickets, deposit items, checks, money orders, cashier's checks, official checks, bank drafts, wire transfer instructions and receipts, checkbooks, check registers, passbooks, withdrawal slips, credit memos, debit memos, signature cards, account applications, automatic teller machine receipts, safe deposit box applications, safe deposit box keys, pre-paid debit and credit cards, debit and credit card statements, charge slips, receipts, financial statements, balance sheets, income statements, cash flow statements, ledgers, journals, accounts receivable, accounts payable, leases, brokerage statements, and any other items evidencing the obtaining, disposition, secreting, transfer, or concealment of assets.

3. Records and information relating to the access and use of money service businesses, such as Western Union and/or Moneygram; online bank transfer services, such as Zelle, Venmo, or Paypal; and cryptocurrency accounts and cryptocurrency exchanges, such as BitCoin.

4. Records and information relating to any communications by, between and among, and/or relating to the SUBJECT PERSON and any conspirators,

[4] As used in this Attachment, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks, backup drives, or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and digital and photographic form.

[5] The SUBJECT PERSON referred to is JONATHAN KING, DOB February 26, 1991.

including but not limited to SMITH and MARTINEZ, relating to the Specified Federal Offenses, including opening and access of bank accounts.

5. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show access, accounts with, and/or use of instant and social media messages (including Facebook, Facebook Messenger, Instagram, Pinterest, Snapchat, FaceTime, Skype, and WhatsApp), SMS and MMS text messages, iMessage, iCloud, and email accounts by the SUBJECT PERSON, and any conspirators, including but not limited to SMITH and MARTINEZ. Records and information showing communications by, between and among, and/or relating to the SUBJECT PERSON, and any conspirators, including but not limited to SMITH and MARTINEZ, that relate to the Specified Federal Offenses via any such accounts and communications platforms.

6. Records and information relating to Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations, including travel to banking locations.

7. Any records which document an association between and among the SUBJECT PERSON, and any conspirators, including but not limited to SMITH and MARTINEZ, including social media accounts, photographs, and video and audio recordings.

8. Records and information records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with any co-conspirators involved in the Specified Federal Offenses, including but not limited to SMITH and MARTINEZ, including calendars, address books, telephone or other contact lists, correspondence, receipts, and wire transfer or fund disposition records, and communications relating to the same.

9. All records or documents evidencing or relating to foreign or domestic travel of the SUBJECT PERSON, or co-conspirators, including but not limited to SMITH and MARTINEZ, including but not limited to airline tickets, tickets for other means of transport, credit card receipts, travel vouchers, hotel receipts, restaurant receipts, gas receipts, notes, schedules, other receipts evidencing travel, boarding passes, itineraries, luggage tags and receipts, frequent flyer statements and awards, car rental receipts and statements, photographs of travel locations, maps, written directions to a location, visas, passports, United States and foreign customs declaration receipts and forms.

10. Records and documents reflecting the purchase or lease of real estate, and vehicles, precious metals, jewelry, or other items obtained with drug trafficking proceeds.

11. Identification cards, driver's license cards, passports, visas, and travel documents.

12. Records relating to the use, ownership, possession, and control of computers, tablets, cellular telephones, including but not limited to the SUBJECT PHONE 2, and/or other cellular and digital devices seized from the SUBJECT PERSON, internet service, or IP addresses associated with the SUBJECT PERSON;

13. For any computer, cellular or digital device, cellular telephone, and/or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information whose seizure is authorized by this warrant, including any cell phones (hereinafter, "DIGITAL DEVICE")[6]:

    a. evidence of who used, owned, or controlled the DIGITAL DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the DIGITAL DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
    e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
    f. evidence of the attachment to the DIGITAL DEVICE of other storage devices or similar containers for electronic evidence;

[6] The term "DIGITAL DEVICE" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, external drives, RAM, flash memory, CD-ROMS, memory sticks, USB drives, and other magnetic or optical media.

g. evidence of programs (and associated data) that are designed to eliminate data from the DIGITAL DEVICE;
h. evidence of the times the DIGITAL DEVICE was used;
i. passwords, encryption keys, and other access devices that may be necessary to access the DIGITAL DEVICE;
j. documentation and manuals that may be necessary to access the DIGITAL DEVICE or to conduct a forensic examination of the DIGITAL DEVICE;
k. records of or information about Internet Protocol addresses used by the DIGITAL DEVICE; and
l. records of or information about the DIGITAL DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

14. With respect to any and all electronically stored information in cellular telephones and cellular devices, in addition to the information described herein, agents may also access, record and seize the following:
h. Telephone numbers of incoming/outgoing calls stored in the call registry;
i. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;
j. Any incoming/outgoing text messages relating to the above criminal violations;
k. Telephone subscriber information;
l. The telephone numbers stored in the cellular telephone and/or PDA;
m. Records relating to the use, possession, and control of any cellular telephones and cellular devices seized;
n. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including but not limited to photographs, videos, e-mail, and voice mail relating to the above Specified Federal Offenses.

15. Contextual information necessary to understand the evidence described in this attachment.

II. AUTHORIZED SEARCH PROCEDURE

1. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

2. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
   a. Any computer or storage medium capable of being used to commit further or store evidence of the Specified Federal Offenses; and
   b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

3. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.

4. This warrant does not cover the search and seizure of any Digital Devices determined by agents to be used exclusively by third parties not involved with the Specified Federal Offenses.

III. SEARCH PROCEDURE FOR DEVICES CAPABLE OF BIOMETRIC ACCESS

1. During the execution of this search warrant, law enforcement is permitted to:
   a. depress the user's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and
   b. hold the device in front of the user's face with her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.